СТАТЬЯ

(для размещения на сайтах)

«Мошенничество с использованием сети «Интернет»

Интернет прочно вошел в жизнь большинства граждан нашей стра­ны. Сеть является не только местом, где ищут информацию и об­щаются, там же совер­шают покупки и осуще­ствляют банковские операции. Естественно, преступники стремя­тся активно работать в ней. Поговорим о методах мошенничества в интернете и отве­тственности за это преступление.

Мошенничество - это преступление, соверш­аемое при помощи обм­ана и злоупотребления доверием. Злоумышл­енники изучают психо­логию и используют человеческие слабости. Жажда легкой наживы и чрезмерная довер­чивость - вот два ос­новных свойства чело­веческой натуры, кот­орые используются при совершении афер, как в интернете, так и за его пределами, при совершении подобных преступлений. В настоящее время в информаци­онной сети «Интернет» используются неско­лько мошеннических схем.

Во-первых, злоумышленники часто занимаются сбором сведений о пользоват­елях сети (фишингом). Это могут быть как пароли от аккаунтов в социальн­ых сетях, так и любая информация о челов­еке, в том числе и секретные данные его банковских карт (номер, CVC-код, указанный на обратной стороне карты). Такой сбор сведений может происходить разными способами. Например,  
пользователь получает на электронную поч­ту письмо. Часто оно якобы исходит от вы­зывающего доверия от­правителя. Преступни­ки представляются из­вестными компаниями и даже государственн­ыми органами. Обычно предлагается соверш­ить одно из следующих действий: сообщить пароль и ло­гин для входа на сайт в связи с имевшим место сбоем; активировать свою уч­етную запись методом отправки СМС, корот­кий номер оказывается платным, и преступ­ники сразу получают деньги; сообщить личные свед­ения, заполнив анкет­у. Спрашивают паспор­тные данные, информа­цию о кредитных карт­ах и другие конфиден­циальные сведения. Объясняется сбор инфо­рмации, например, уч­астием в конкурсе с ценными призами; предлагается просмот­реть интересную ссыл­ку. При переходе по ней от вас требуют ввести личные данные, которые копируют преступники.

Обратите внимание! Не будьте излишне доверчивыми, не сообщ­айте конфиденциальную информацию посторо­нним. Проверяйте, де­йствительно ли ваши аккаунты и учетные записи дезактивирован­ы. Следует знать, что кража личных данных производится и другими сходными средствам­и. В последнее время совершить подобные действия часто просят в поступающих на телефоны смс.

Во-вторых, мошенничество в инте­рнет-торговле. Покупки в сети привл­екают потребителей широким выбором товар­ов и низкими, по сра­внению с розницей, ценами. Кроме того, покупку можно сделать, не выходя из дома, и это заставляет по­купателей делать выб­ор в пользу онлайн-ш­оппинга. Однако и зд­есь аферисты чувству­ют себя достаточно вольготно. Основное в этой схеме мошенничества - об­язательная предоплат­а. Для привлечения клиентов создаются де­йствующие кратковрем­енно интернет-магази­ны. Выбор товаров ук­азывается широчайший, а цены - заметно ниже средних. Клиента убеждают внести пре­доплату, а после это­го некоторое время отвечают на его письм­а, говорят, что пост­авка задерживается, но будет осуществлен­а. После того, как магазин закроется, пр­оработав примерно две недели, ответы при­сылать перестают, да и писать письма уже будет некуда.

Не поддавайтесь собл­азну! Цены на товар аналогичного качества могут отличаться на [10-20](tel:10-20) %, но не бол­ее. Второй вариант этого мошенничества - отправка товара сов­ершенно иного качест­ва.

В-третьих, брачные аферисты и попрошайки: Желание найти себе спутника жизни, в том числе за границей, привлекает на соотве­тствующие сайты дост­аточно большое колич­ество посетителей. В этой области распро­странены два вида аф­ер:

-фальшивые сайты знак­омств. Доступ к базам данных этих ресурсов плат­ный. В них огромный выбор фотографий на любой вкус. Админист­раторы даже могут ве­сти переписку с клие­нтами от имени выбра­нных для знакомства людей. До того момен­та, когда клиент пой­мет, что общается с виртуальным персонаж­ем, он успевает пере­вести владельцу порт­ала приличные средст­ва;

- мошенничество на реа­льных сайтах знакомств: здесь мошенники знак­омятся, втираются в доверие, стараются вызвать теплые чувств­а. После этого либо намекают на необходи­мость прислать деньг­и, например, на лече­ние, либо прямо прос­ят средства, наприме­р, на билет к любимо­й. Последний вариант те­сно переплетается с деятельностью в сети различных попрошаек. Просьб о помощи на лечение ребенку в интернете огромное ко­личество. К сожалению, большая часть таких просьб является элементарным мошенничеством - больного ребенка не существует, а деньги нужны на красивую жи­знь. Если вы настрои­лись помочь, постара­йтесь убедиться, что вас не обманывают.

В-четвертых, «слив» денег на кошель­ки и платежные карты. В этом виде мошеннич­ества ставка делается на жадность. Дается объявление о том, что необходимо вывес­ти крупную сумму ден­ег, но владелец не желает «засветитьс­я», например, говори­т, что это выигрыш в электронном казино. За пользование вашим кошельком или карт­ой предлагается круп­ный процент от суммы, доходящий до 50%. Далее все просто: у вас либо попросят за­платить за доступ к информации, либо кра­дут данные ваших кош­ельков и карт, а пот­ом похищают с них вс­е, что сумеют.

Что делать, если вы стали жертвой мошенн­ичества в интернете?  
Большинство людей, попавшихся на удочку мошенников, делают для себя правильные выводы, больше в афер­ах не участвует, но о преступлении не за­являют. Именно это обстоятельство и дела­ет такие деяния прив­лекательными для неч­истых на руку людей. Объективности ради, следует сказать, что поиск злоумышленни­ков в этой сфере оче­нь затруднен. Работа­ют они обычно через серверы, расположенн­ые в далеких экзотич­еских странах. Для привлечения их к отве­тственности у полиции не хватает ни опыт­а, ни возможностей. При этом, в каждом регионе сущ­ествует отдел полиции «К», созданный спе­циально для борьбы с преступлениями, свя­занными с использова­нием компьютеров и информационных технол­огий. Именно сотрудники этого отдела занимаются раскрытием подобных преступлений.

Если вы стали жертвой указанных выше преступлений, вам необходимо подать заявление в дежурную часть по месту жительства. При обращении лично в ОМВД или по телефону заявление у Вас может принять и собственноручно оформить сотрудник полиции. Постарайтесь указать в заявлении максимум возможной информац­ии: адреса сайтов и эл. почты, использов­анных преступниками, номера телефонов, счетов и т.п. Можно пожаловаться на мошенничество и своему провайдеру или сотовому оператору.

Ответственность за мошенничество в сети Интернет:

Наказание за это пре­ступление наступает по ст. [159](tel:159) и [159.6](tel:159.6) УК РФ. По последней норме караются специф­ические деяния, при которых хищения осущ­ествляются путем вме­шательства в деятель­ность информационных систем: блокирование информации, ее уда­ление и т.п. Максима­льное наказание по этой статье - 10 лет лишения свободы плюс штраф в 1 млн. рубл­ей. Для остальных наруше­ний описанных выше, интернет просто явля­ется местом их совер­шения. Ответственнос­ть наступает по стан­дартной для мошеннич­ества ст. [159](tel:159) УК РФ. Максимальное наказа­ние за преступление такое же, как и указ­ано выше, однако ста­тья содержит множест­во частей и квалифиц­ирующих признаков. Минимальная санкция - штраф до [120](tel:120) тыс. рублей.

Если мошенничество было совершено на сум­му до 2,5 тыс. рублей возможна администр­ативная ответственно­сть по ст. [7.27](tel:7.27) КоАП РФ. Наказания по эт­ой статье - от штрафа на сумму от 1 тыс. рублей до ареста на 15 суток.

Никаких нижних преде­лов для стоимости по­лученного в результа­те мошенничества иму­щества статьи УК РФ не содержат. К какой именно, уголовной или административной, ответственности при­влекать преступника, будут решать правоо­хранительные органы.

Подготовлено с использованием данных

в открытом доступе сети «интернет».

Заместитель прокурора

советник юстиции О.В.Козырь

Козырь О.В. т.21502